#6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|---|---|---|
| In re application of | : | **Confirmation No. 8418** |
| Masato YAMAMICHI et al. | : | Docket No. 2001_1845A |
| Serial No. 10/020,308 | : | Group Art Unit 2131 |
| Filed December 18, 2001 | : | |

CRYPTOCOMMUNICATION SYSTEM,
TRANSMISSION APPARATUS,
AND RECEPTION APPARATUS

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

---

**CLAIM OF PRIORITY UNDER 35 USC 119**

Assistant Commissioner for Patents,
Washington, DC 20231

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2000-384835, filed December 19, 2000, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Masato YAMAMICHI et al.

By _____
Michael S. Huppert
Registration No. 40,268
Attorney for Applicants

MSH/kjf
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
April 30, 2002

CERTIFIED COPY OF
PRIORITY DOCUMENT

# 日本国特許庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月１９日

出願番号
Application Number: 特願２０００－３８４８３５

出願人
Applicant(s): 松下電器産業株式会社

２００１年１１月 ２日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願

【整理番号】　2022520534

【提出日】　平成12年12月19日

【あて先】　特許庁長官殿

【国際特許分類】　G09C　5/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　山道　将人

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　布田　裕一

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　大森　基司

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　館林　誠

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　データ暗号化システム、暗号装置、及び復号装置

【特許請求の範囲】

【請求項１】送信側と受信側で、予め対となる暗号鍵と復号鍵、また一方向性関数を定めておき、

送信側で、平文を、前記暗号鍵と前記一方向性関数に基づいて、暗号化して、暗号文を生成し、暗号文を受信側に送信し、

受信側では、前記暗号文を、前記復号鍵と一方向性関数に基づいて、復号し、復号文を入手するデータ暗号化システムであって、

前記送信側では、

前記平文を、前記暗号鍵に基づいて、暗号化部により暗号化し、第１の暗号部分情報を生成し、

前記平文を、前記一方向性関数に基づいて、第１の一方向性関数部により第２の暗号部分情報を生成し、

前記第１の暗号部分情報と前記第２の暗号部分情報を連結して、暗号文として前記受信側に送信する暗号装置を備え、

前記受信側では、

受信した前記暗号文のうち前記第１の暗号部分情報を、前記復号鍵に基づいて、復号化部により復号し、第１の復号部分情報を生成し、

前記第１の復号部分情報を、前記一方向性関数に基づいて、前記第１の一方向性関数部と同じ動作を行う第２の一方向性関数部により第２の復号部分情報を生成し、

前記第２の復号部分情報が前記第２の暗号部分情報と等しい場合は、前記第１の復号部分情報を復号文とする復号装置を備えることを特徴とするデータ暗号化システム。

【請求項２】平文を、前記暗号鍵に基づいて、暗号化部により暗号化し、第１の暗号部分情報を生成し、前記平文を、前記一方向性関数に基づいて、第１の一方向性関数部により第２の暗号部分情報を生成し、前記第１の暗号部分情報と前記第２の暗号部分情報を連結して、暗号文として送信することを特徴とする請求

項１に記載の暗号装置。

【請求項３】受信した暗号文のうち第１の暗号部分情報を、請求項１に記載の復号鍵に基づいて、復号化部により復号し、第１の復号部分情報を生成し、前記第１の復号部分情報を、前記一方向性関数に基づいて、前記第１の一方向性関数部と同じ動作を行う第２の一方向性関数部により第２の復号部分情報を生成し、前記第２の復号部分情報が受信した暗号文のうちの第２の暗号部分情報と等しい場合は、前記第１の復号部分情報を復号文とすることを特徴とする請求項１に記載の復号装置。

【請求項４】送信側と受信側で、予め対となる暗号鍵と復号鍵、また一方向性関数を定めておき、

送信側で、平文を、前記暗号鍵と一方向性関数に基づいて、暗号化して、暗号文を生成し、暗号文を受信側に送信し、

受信側では、前記暗号文を、前記復号鍵と前記一方向性関数に基づいて、復号し、復号文を入手するデータ暗号化システムであって、

前記送信側では、

前記平文に、情報付加部により付加情報を付加し、中間情報を生成し、

前記中間情報を、前記暗号鍵に基づいて、暗号化部により暗号化し、第１の暗号部分情報を生成し、

前記平文を、前記一方向性関数に基づいて、第１の一方向性関数部により第２の暗号部分情報を生成し、

前記第１の暗号部分情報と前記第２の暗号部分情報を連結して、暗号文として前記受信側に送信する暗号装置を備え、

前記受信側では、

受信した前記暗号文のうち前記第１の暗号部分情報を、前記復号鍵に基づいて、復号化部により復号し、第１の復号部分情報を生成し、

前記第１の復号部分情報から、情報除去部により前記付加情報を除去し、第２の復号部分情報を生成し、

前記第２の復号部分情報を、前記一方向性関数に基づいて、前記第１の一方向性関数部と同じ動作を行う第２の一方向性関数部により第３の復号部分情報を生

成し、

前記第３の復号部分情報が前記第２の暗号部分情報と等しい場合は、前記第２の復号部分情報を復号文とする復号装置を備えることを特徴とするデータ暗号化システム。

【請求項５】平文に、情報付加部により付加情報を付加し、中間情報を生成し、前記中間情報を、前記暗号鍵に基づいて、暗号化部により暗号化し、第１の暗号部分情報を生成し、前記中間情報を、前記一方向性関数に基づいて、第１の一方向性関数部により第２の暗号部分情報を生成し、前記第１の暗号部分情報と前記第２の暗号部分情報を連結して、暗号文として送信することを特徴とする請求項４に記載の暗号装置。

【請求項６】受信した暗号文のうち第１の暗号部分情報を、前記復号鍵に基づいて、復号化部により復号し、第１の復号部分情報を生成し、前記第１の復号部分情報から、情報除去部により前記付加情報を除去し、第２の復号部分情報を生成し、前記第２の復号部分情報を、前記一方向性関数に基づいて、前記一方向性関数部と同じ動作を行う第２の一方向性関数部により、第３の復号部分情報を生成し、前記第３の復号部分情報が受信した暗号文のうちの第２の暗号部分情報と等しい場合は、前記第２の復号部分情報を復号文とすることを特徴とする請求項４に記載の復号装置。

【請求項７】前記暗号化部で用いられる暗号方式は、公開鍵暗号方式であることを特徴とする請求項１または請求項４に記載のデータ暗号化システム。

【請求項８】前記第１の一方向性関数部で用いられる一方向性関数はハッシュ関数であることを特徴とする請求項１または請求項４に記載のデータ暗号化システム。

【請求項９】前記第１の一方向性関数部で用いられる一方向性関数は、秘密鍵暗号方式の暗号化関数であることを特徴とする請求項１または請求項４に記載のデータ暗号化システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、復号時の誤り検出技術に関するものである。

【０００２】

【従来の技術】

秘匿通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行う方式である。暗号方式とは、この秘匿通信方式を実現するための一つの手段であり、簡単に説明すると、平文を暗号化するための暗号化アルゴリズムと暗号鍵、及び暗号文を復号するための復号アルゴリズムと復号鍵が存在して、暗号化アルゴリズムと暗号鍵を用いて平文を暗号化して送信し、復号アルゴリズムと復号鍵を用いて受信された暗号文を復号して復号文を得る方式である。暗号化アルゴリズムは、平文を入力として暗号文を出力するので、暗号化関数とも呼ばれる。また、復号アルゴリズムは、暗号文を入力として復号文を出力するので、復号化関数とも呼ばれる。暗号方式については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書に詳しく述べられている。

【０００３】

暗号方式の中に、正規の暗号鍵を用いて暗号化した暗号文を、正規の復号鍵を用いて復号しても、復号により得られた復号文が平文ｍと異なる可能性がある暗号方式がある。以降、正規の復号鍵を用いて復号しても、復号文が平文ｍと異なることを、「復号誤り」と記述し、復号誤りが生じる可能性がある暗号方式を、「復号誤りが発生し得る暗号方式」と記述する。

【０００４】

上記復号誤りが発生し得る暗号方式として、例えば、ＮＴＲＵ暗号方式がそれにあたる。この方式を簡単に説明すると、暗号鍵を用いて、平文を乱数をパラメータとして暗号化して暗号文を生成し、復号鍵を用いて、暗号文を復号して復号文を生成する方式である。この方式は、乱数をパラメータとして暗号化するので、平文が同じでも暗号文が異なる可能性があり、また、復号誤りが発生し得る方式である。ＮＴＲＵ暗号方式については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, “NTRU: A ring based public key cryptosystem”,Lecture Notes in Computer Science, 1423, pp.267-288,Springer-Verlag, 1998.

に詳しく述べられている。復号誤りが発生し得る暗号方式の一つであるＮＴＲＵ暗号方式において、暗号鍵Ｋｐを用いて暗号化する際に、乱数ｒをパラメータとして、平文ｍを暗号化した暗号文ｃを生成する関数をＥで表し、入力ｍ，Ｋｐ，ｒに対する出力がｃであることを、

ｃ＝Ｅ（ｍ，Ｋｐ，ｒ）

で表す。また、復号鍵Ｋｓを用いて、暗号文ｃから復号文ｍ’を生成する関数をＤで表し、入力ｃ，Ｋｓに対する出力がｍ’であることを、

ｍ’＝Ｄ（ｃ，Ｋｓ）

で表す。

【０００５】

（従来例１）

以下に、上記復号誤りが発生し得る暗号方式を用いたデータ暗号化システム３０００について、ＮＴＲＵ暗号方式を例として、図１１～図１５を用いて説明する。図１１はデータ暗号化システム３０００のブロック図であり、図１２は暗号装置３１００のブロック図であり、図１３は暗号化部３１１０のブロック図であり、図１４は復号装置３２００のブロック図であり、図１５は復号化部３２１０のブロック図である。暗号装置３１００及び復号装置３２００は、通信路３３００、例えば、無線通信路やインターネットなどで接続されているものとする。

【０００６】

またＮＴＲＵ暗号方式については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, “NTRU: A ring based public key cryptosystem” ,Lecture Notes in Computer Science, 1423, pp.267-288,Springer-Verlag, 1998.に詳しく述べられている。

【０００７】

（１）鍵の生成

上記暗号方式を用いた通信を行う前に、適切な方法で上記暗号方式における復号鍵Ｋｓ、及び暗号鍵Ｋｐが生成されて、復号鍵Ｋｓは復号化部３２１０に格納され、暗号鍵Ｋｐは暗号化部３１１０に格納されているものとする。復号鍵Ｋｓ、及び暗号鍵Ｋｐの生成方法は、上記文献に述べられている。

【０００８】

（２）暗号文の生成及び送信（暗号装置３１００の処理）

暗号化部３１１０は、ＮＴＲＵ暗号方式の暗号化を行うものであり、乱数生成部３１１２で乱数ｒを生成し、予め格納されている暗号鍵Ｋｐを用いて、平文ｍを暗号化関数部３１１１で、乱数ｒをパラメータとして暗号化し、暗号文ｃを生成する。即ち、

ｃ＝Ｅ（ｍ，Ｋｐ，ｒ）

そして、生成した暗号文ｃを送信部３１２０により、通信路３３００へ送信する。

【０００９】

（３）暗号文の受信及び復号（復号装置３２００の処理）

受信部３２２０は通信路３３００から暗号文ｃを受信し、これを復号化部３２１０に送る。復号化部３２１０は、ＮＴＲＵ暗号方式の復号を行うものであり、予め格納されている復号鍵Ｋｓを用いて、受信した暗号文ｃを、復号化関数部３２１１で復号し、復号文ｍ’を得る。即ち、

ｍ’＝Ｄ（ｃ，Ｋｓ）

上記従来例１に示した復号誤りが発生し得る暗号方式を用いた暗号通信では、復号装置３２００が暗号文を復号したときに、復号誤りのために暗号装置３１００に入力された平文ｍを得られない場合がある。つまり、

ｍ’＝Ｄ（Ｅ（ｍ，Ｋｐ，ｒ），Ｋｓ）

とすると、復号誤りの発生のために、ｍ’≠ｍとなる場合がある。

【００１０】

復号誤りが発生しなかった場合、復号装置３２００は受信した暗号文ｃから暗号装置３１００に入力された平文ｍを出力することができるが、復号誤りが発生した場合、復号装置３２００は、暗号装置３１００に入力された平文ｍとは別のものを得ることになる。

【００１１】

ここで、復号装置３２００は、復号誤りの発生の有無に関わらず、暗号文ｃから何らかの復号文ｍ’を出力することができるが、果たしてそれが暗号装置３１

００に入力された平文ｍと同一であるかどうかを判断することができない。つまり、受け取った暗号文を復号しても、その復号文は信頼がおけるかどうかを、復号装置を用いて判定できないことになる。

【００１２】

このように、この例では、復号装置は、受信した暗号文から得られた復号文ｍ’が、暗号装置３１００に入力された平文ｍと同一であるかどうか判定できないため、データ暗号化システム３０００においては意図した情報を確実に伝えることができないという問題がある。

【００１３】

（従来例２）

以下に、従来例１の上記問題を解決するための復号誤りが発生し得る暗号方式を用いたデータ暗号化システム４０００について、ＮＴＲＵ暗号方式を例として、図１６～図２０を用いて説明する。図１６はデータ暗号化システム４０００のブロック図であり、図１７は暗号装置４１００のブロック図であり、図１８は暗号化部４１１０のブロック図であり、図１９は復号装置４２００のブロック図であり、図２０は復号化部４２１０のブロック図である。暗号装置４１００、及び復号装置４２００は、通信路４３００で接続されている。

【００１４】

（１）鍵の生成

上記暗号方式を用いた通信を行う前に、適切な方法で上記暗号方式における復号鍵Ｋｓ、及び暗号鍵Ｋｐが生成されて、復号鍵Ｋｓは復号化部４２１０に格納され、暗号鍵Ｋｐは暗号化部４１１０に格納されているものとする。復号鍵Ｋｓ、及び暗号鍵Ｋｐの生成方法は、上記文献に述べられている。

【００１５】

（２）暗号文の生成及び送信（暗号装置４１００の処理）

暗号化部４１１０は、ＮＴＲＵ暗号方式の暗号化を行うものであり、乱数生成部４１１２で乱数ｒを生成し、予め格納されている暗号鍵Ｋｐを用いて、平文ｍを暗号化関数部４１１１で、乱数ｒをパラメータとして暗号化し、暗号文ｃ＝Ｅ（ｍ，Ｋｐ，ｒ）を生成するものである。

【００１６】

暗号装置４１００は、平文ｍを暗号化部４１１０によりｎ回（ｎは２以上の整数）暗号化して、ｎ個の暗号文ｃ［１］，ｃ［２］，・・・，ｃ［ｎ］を生成する。即ち、

ｃ［１］＝Ｅ（ｍ，Ｋｐ，ｒ［１］）

ｃ［２］＝Ｅ（ｍ，Ｋｐ，ｒ［２］）

・・・

ｃ［ｎ］＝Ｅ（ｍ，Ｋｐ，ｒ［ｎ］）

ここでｒ［１］，ｒ［２］，・・・，ｒ［ｎ］は、上記乱数生成部４１１２で生成される乱数とする。そして、生成したｎ個の暗号文ｃ［１］，ｃ［２］，・・・，ｃ［ｎ］を送信部４１２０により、通信路４３００へ送信する。

【００１７】

（３）暗号文の受信及び復号（復号装置４２００の処理）

受信部４２２０は、暗号文ｃ［１］，ｃ［２］，・・・，ｃ［ｎ］を受信し、これらを復号化部４２１０に送る。復号化部４２１０は、ＮＴＲＵ暗号方式の復号を行うものであり、予め格納されている復号鍵Ｋｓを用いて、受信した暗号文ｃ［１］，ｃ［２］，・・・，ｃ［ｎ］を、それぞれ復号化関数部４２１１で復号し、復号文ｍ’［１］，ｍ’［２］，・・・，ｍ’［ｎ］を得る。即ち、

ｍ’［１］＝Ｄ（ｃ［１］，Ｋｓ）

ｍ’［２］＝Ｄ（ｃ［２］，Ｋｓ）

・・・

ｍ’［ｎ］＝Ｄ（ｃ［ｎ］，Ｋｓ）

（４）復号誤りの検出

復号装置４２００は比較部４２３０を用いて、上記のようにして得られた復号文ｍ’［１］，ｍ’［２］，・・・，ｍ’［ｎ］が一つでも異なっていたら復号誤りが発生したとみなし、ｊ＝０、それ以外はｊ＝１とし、ｍ’［１］，ｍ’［２］，・・・，ｍ’［ｎ］，ｊを出力する。

【００１８】

上記の従来例２は、従来例１に比べ、復号誤りを検出できるという利点がある

。しかし、この方法を用いると、通信量が従来例１のｎ倍になり、非効率的である。さらに、異なる乱数をパラメータとして同じ平文を暗号化した複数の暗号文を送信することにより、暗号方式の安全性が低下する恐れもある。これは、

ｃ［１］＝Ｅ（ｍ，Ｋｐ，ｒ［１］）

ｃ［２］＝Ｅ（ｍ，Ｋｐ，ｒ［２］）

・・・

ｃ［ｎ］＝Ｅ（ｍ，Ｋｐ，ｒ［ｎ］）

のｎ個の関係式から平文ｍや乱数ｒ［１］，ｒ［２］，・・・，ｒ［ｎ］に関する情報が第三者に漏れる恐れがあるからである。このことを利用した暗号攻撃法を、Multiple Transmission Attackと言う。

【００１９】

具体的には、復号誤りの発生し得る暗号方式の１つであるＮＴＲＵ暗号方式を用いて、上記復号誤り検出を行うと安全性が低下することが知られている。この攻撃法については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, “NTRU: A ring based public key cryptosystem” ,Lecture Notes in Computer Science,1423,pp.267-288,Springer-Verlag, 1998.に詳しく述べられている。

【００２０】

【発明が解決しようとする課題】

暗号システムにおいて、平文を相手に正しく伝えることが重要なのは言うまでもない。復号誤りの発生し得る暗号方式においては、復号誤りを検出することが最低限必要である。従来技術においては、復号誤りを検出しようとすると、通信量が増大し、しかも安全性が低下する恐れもある。

【００２１】

本発明は、以上の従来技術における問題点を鑑みて行われたもので、データ暗号化システムにより、安全で効率的に復号誤りを検出する技術を提供することを目的とする。

【００２２】

【課題を解決するための手段】

上記課題を解決するために、請求項１における発明は、送信側と受信側で、予め対となる暗号鍵と復号鍵、また一方向性関数を定めておき、送信側で、平文を、前記暗号鍵と一方向性関数に基づいて、暗号化して、暗号文を生成し、暗号文を受信側に送信し、受信側では、前記暗号文を、前記復号鍵と前記一方向性関数に基づいて、復号し、復号文を入手するデータ暗号化システムであって、前記送信側では、前記平文を、前記暗号鍵に基づいて、暗号化部により暗号化し、第１の暗号部分情報を生成し、前記平文を、前記一方向性関数に基づいて、第１の一方向性関数部により第２の暗号部分情報を生成し、前記第１の暗号部分情報と前記第２の暗号部分情報を連結して、暗号文として前記受信側に送信する暗号装置を備え、前記受信側では、受信した前記暗号文のうち前記第１の暗号部分情報を、前記復号鍵に基づいて、復号化部により復号し、第１の復号部分情報を生成し、前記第１の復号部分情報を、前記一方向性関数に基づいて、前記第１の一方向性関数部と同じ動作を行う第２の一方向性関数部により第２の復号部分情報を生成し、前記第２の復号部分情報が前記第２の暗号部分情報と等しい場合は、前記第１の復号部分情報を復号文とする復号装置を備えることを特徴とする。

【００２３】

請求項２における発明は、請求項１に記載の暗号装置は、平文を、請求項１に記載の暗号鍵に基づいて、暗号化部により暗号化し、第１の暗号部分情報を生成し、前記平文を、請求項１に記載の一方向性関数に基づいて、第１の一方向性関数部により第２の暗号部分情報を生成し、前記第１の暗号部分情報と前記第２の暗号部分情報を連結して、暗号文として送信することを特徴とする。

【００２４】

請求項３における発明は、請求項１に記載の復号装置は、受信した暗号文のうち第１の暗号部分情報を、請求項１に記載の復号鍵に基づいて、復号化部により復号し、第１の復号部分情報を生成し、前記第１の復号部分情報を、請求項１に記載の一方向性関数に基づいて、請求項１に記載の第１の一方向性関数部と同じ動作を行う第２の一方向性関数部により第２の復号部分情報を生成し、前記第２の復号部分情報が受信した暗号文のうちの第２の暗号部分情報と等しい場合は、前記第１の復号部分情報を復号文とすることを特徴とする。

【００２５】

請求項４における発明は、送信側と受信側で、予め対となる暗号鍵と復号鍵、また一方向性関数を定めておき、送信側で、平文を、前記暗号鍵と一方向性関数に基づいて、暗号化して、暗号文を生成し、暗号文を受信側に送信し、受信側では、前記暗号文を、前記復号鍵と前記一方向性関数に基づいて、復号し、復号文を入手するデータ暗号化システムであって、前記送信側では、前記平文に、情報付加部により付加情報を付加し、中間情報を生成し、前記中間情報を、前記暗号鍵に基づいて、暗号化部により暗号化し、第１の暗号部分情報を生成し、前記平文を、前記一方向性関数に基づいて、第１の一方向性関数部により第２の暗号部分情報を生成し、前記第１の暗号部分情報と前記第２の暗号部分情報を連結して、暗号文として前記受信側に送信する暗号装置を備え、前記受信側では、受信した前記暗号文のうち前記第１の暗号部分情報を、前記復号鍵に基づいて、復号化部により復号し、第１の復号部分情報を生成し、前記第１の復号部分情報から、情報除去部により前記付加情報を除去し、第２の復号部分情報を生成し、前記第２の復号部分情報を、前記一方向性関数に基づいて、前記第１の一方向性関数部と同じ動作を行う第２の一方向性関数部により第３の復号部分情報を生成し、前記第３の復号部分情報が前記第２の暗号部分情報と等しい場合は、前記第２の復号部分情報を復号文とする復号装置を備えることを特徴とする。

【００２６】

請求項５における発明は、請求項４に記載の暗号装置は、平文に、情報付加部により付加情報を付加し、中間情報を生成し、前記中間情報を、請求項４に記載の暗号鍵に基づいて、暗号化部により暗号化し、第１の暗号部分情報を生成し、前記中間情報を、請求項４に記載の一方向性関数に基づいて、第１の一方向性関数部により第２の暗号部分情報を生成し、前記第１の暗号部分情報と前記第２の暗号部分情報を連結して、暗号文として送信することを特徴とする。

【００２７】

請求項６における発明は、請求項４に記載の復号装置は、受信した暗号文のうち第１の暗号部分情報を、請求項４に記載の復号鍵に基づいて、復号化部により復号し、第１の復号部分情報を生成し、前記第１の復号部分情報から、情報除去

部により前記付加情報を除去し、第２の復号部分情報を生成し、前記第２の復号部分情報を、請求項４に記載の一方向性関数に基づいて、請求項４に記載の第１の一方向性関数部と同じ動作を行う第２の一方向性関数部により、第３の復号部分情報を生成し、前記第３の復号部分情報が受信した暗号文のうちの第２の暗号部分情報と等しい場合は、前記第２の復号部分情報を復号文とすることを特徴とする。

【００２８】

請求項７における発明は、請求項１または請求項４に記載のデータ暗号化システムは、暗号化部で用いられる暗号方式が、公開鍵暗号方式であることを特徴とする。

【００２９】

請求項８における発明は、請求項１または請求項４に記載のデータ暗号化システムは、第１の一方向性関数部で用いられる一方向性関数が、ハッシュ関数であることを特徴とする。

【００３０】

請求項９における発明は、請求項１または請求項４に記載のデータ暗号化システムは、第１の一方向性関数部で用いられる一方向性関数が、秘密鍵暗号方式の暗号化関数であることを特徴とする。

【００３１】

【発明の実施の形態】

（実施の形態１）

図１は、実施の形態１における復号誤りが発生し得る暗号方式における復号誤り検出が可能であるデータ暗号化システム１０００の構成を示すブロック図である。

【００３２】

（データ暗号化システム１０００の構成）

データ暗号化システム１０００は、復号誤りが発生し得る暗号方式における復号誤り検出が可能であるシステムであり、暗号装置１１００、復号装置１２００、及び通信路１３００から構成される。ここでは、復号誤りが発生し得る暗号方

式として、ＮＴＲＵ暗号方式を用いた構成例を与える。ＮＴＲＵ暗号、及びＮＴＲＵ暗号方式の暗号鍵、及び復号鍵の生成方法については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, “NTRU: A ring based public key cryptosystem” ,Lecture Notes in Computer Science, 1423, pp.267-288,Springer-Verlag, 1998.に詳しく述べられている。

【００３３】

（暗号装置１１００の構成）

図２は、暗号装置１１００の構成を示すブロック図である。暗号装置１１００は、暗号化部１１１０、第１の一方向性関数部１１２０、及び送信部１１３０を備える。ここでは、暗号化部１１１０としてＮＴＲＵ暗号方式を用い、第１の一方向性関数部１１２０としてハッシュ関数を用いた構成例を与える。暗号装置１１００は、平文ｍを入力とし、ｍに対する第１の暗号部分情報であるＮＴＲＵ暗号方式による暗号文ｃ（＝Ｅ（ｍ，Ｋｐ，ｒ））と、第２の暗号部分情報であるハッシュ関数値ｈ（ｍ）を連結して出力する。

【００３４】

（暗号化部１１１０）

図３は、暗号化部１１１０の構成を示すブロック図である。暗号化部１１１０は、ＮＴＲＵ暗号方式の暗号化を行うものであり、暗号化関数部１１１１、及び乱数生成部１１１２を備え、予め暗号化に用いる暗号鍵Ｋｐが与えられているものとする。暗号化部１１１０は、入力として平文ｍが与えられたとき、乱数生成部１１１２で乱数ｒを生成し、予め与えられた暗号鍵Ｋｐを用いて暗号化する際に、乱数ｒをパラメータとして使用して、平文ｍを暗号化関数部１１１１で暗号化した結果Ｅ（ｍ，Ｋｐ，ｒ）を生成し、送信部１１３０に入力する。以下、実施の形態１において、

ｃ＝Ｅ（ｍ，Ｋｐ，ｒ）

とする。ここで、上記乱数の例としては、Ｃ言語のライブラリ関数であるｒａｎｄ（）が挙げられる。

【００３５】

（第１の一方向性関数部１１２０）

第１の一方向性関数部１１２０は、予め一方向性関数としてハッシュ関数ｈが与えられているものとする。第１の一方向性関数部１１２０は、上記平文ｍのハッシュ関数ｈの値ｈ（ｍ）を生成し、送信部１１３０に入力する。

【００３６】

ここで、一方向性関数とは、関数値を計算することは容易であるが、関数値から関数に入力された元の値を求めることが困難な関数のことである。また、ここで用いるハッシュ関数ｈは、関数の値ｈ（ｍ）から平文ｍの値を得ることが困難であるような十分に安全なもので、かつ衝突困難なものとする。一方向性関数、ハッシュ関数、ハッシュ関数の安全性、及びハッシュ関数の衝突困難性については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書、１９９７、５６ページ及び１８９～１９５ページに詳しく述べられている。

【００３７】

（送信部１１３０）

送信部１１３０は、暗号化部１１１０から入力された暗号文ｃと第１の一方向性関数部１１２０から入力されたｈ（ｍ）を連結して通信路１３００に送信する。

【００３８】

（復号装置１２００の構成）

図４は、復号装置１２００の構成を示すブロック図である。復号装置１２００は、入力として暗号文ｃとハッシュ関数値ｈ（ｍ）を受け取り、復号文ｍ’（＝Ｄ（ｃ，Ｋｓ））と復号誤り検出結果ｊを出力する。復号装置１２００は、復号化部１２１０、第２の一方向性関数部１２２０、受信部１２３０、及び比較部１２４０を備える。

【００３９】

（復号化部１２１０）

図５は、復号化部１２１０の構成を示すブロック図である。復号化部１２１０は、暗号化部１１１０で用いられた暗号方式の復号を行うものであり、復号化関数部１２１１を備え、予め復号に用いる復号鍵Ｋｓが与えられているものとする。復号化部１２１０は、入力として上記暗号文ｃが与えられたとき、予め与えら

れた復号鍵Ｋｓを用いて、暗号文ｃを復号化関数部１２１１で復号した結果Ｄ（ｃ，Ｋｓ）を生成し、第２の一方向性関数部１２２０に入力する。以下、実施の形態１において、

ｍ’＝Ｄ（ｃ，Ｋｓ）

とする。

【００４０】

（第２の一方向性関数部１２２０）

第２の一方向性関数部１２２０は、第１の一方向性関数部１１２０と同じ動作を行うものであり、予め一方向性関数としてハッシュ関数ｈが与えられているものとする。第２の一方向性関数部１２２０は、上記復号結果ｍ’のハッシュ関数ｈの値ｈ（ｍ’）を生成し、比較部１２４０に入力する。

【００４１】

（受信部１２３０）

受信部１２３０は、通信路１３００から連結された入力ｃ，ｈ（ｍ）を受け取り、ｃを復号化部１２１０に、ｈ（ｍ）を比較部１２４０にそれぞれ入力する。

【００４２】

（比較部１２４０）

比較部１２４０は、ｈ（ｍ）とｈ（ｍ’）を入力として、ｈ（ｍ）とｈ（ｍ’）が等しいかどうか比較し、等しい場合はｊ＝１とし、等しくない場合はｊ＝０をとして、比較結果ｊを出力する。

【００４３】

（通信路１３００の構成）

通信路１３００は、暗号装置１１００と復号装置１２００との間のデータのやり取りが可能であるような通信路である。例えば、無線通信路やインターネットである。

【００４４】

（データ暗号化システム１０００の動作）

データ暗号化システム１０００の全体の動作について、図１、図２、図４と、以下に述べる処理順序を用いて説明する。ここで、暗号鍵Ｋｐ、復号鍵Ｋｓ、及

び一方向性関数ｈは予め適切な方法で生成され、暗号鍵Ｋｐは暗号化部１１１０に格納され、復号鍵Ｋｓは復号化部１２１０に格納され、一方向性関数ｈは第１の一方向性関数部１１２０及び第２の一方向性関数部１２２０に与えられているものとする。

【００４５】

暗号装置１１００は、入力として平文ｍを受け取る（ステップＳ１０１）。暗号化部１１１０は、入力されたｍに対し、ｃ＝Ｅ（ｍ，Ｋｐ，ｒ）を生成し、送信部１１３０に入力する（ステップＳ１０２）。第１の一方向性関数部１１２０は、入力されたｍに対し、ｈ（ｍ）を生成し、送信部１１３０に入力する（ステップＳ１０３）。送信部１１３０は、入力されたｃ、及びｈ（ｍ）を連結して暗号文とし、通信路１３００に送信する（ステップＳ１０４）。

【００４６】

受信部１２３０は、通信路１３００から暗号文である連結されたｃ、及びｈ（ｍ）を受信し、ｃを復号化部１２１０に、ｈ（ｍ）を比較部１２４０にそれぞれ入力する（ステップＳ１０５）。復号化部１２１０は、入力されたｃに対し、ｍ’＝Ｄ（ｃ，Ｋｓ）を生成し、第２の一方向性関数部１２２０に入力する（ステップＳ１０６）。第２の一方向性関数部１２２０は、入力されたｍ’に対し、ｈ（ｍ’）を生成し、比較部１２４０に入力する（ステップＳ１０７）。比較部１２４０は、入力されたｈ（ｍ’）とｈ（ｍ）が等しいかどうかを判定し、等しい場合はｊ＝１とし、等しくない場合はｊ＝０として、比較結果ｊを出力する（ステップＳ１０８）。

【００４７】

復号装置１２００は、復号化部１２１０で出力されたｍ’と比較部１２４０で出力されたｊを復号文として出力する（ステップＳ１０９）。

【００４８】

（実施の形態１における動作検証と従来例との比較）

以下に、この例の復号誤りの検出について説明する。以下で従来の方法との比較を行う。この例では、復号誤りが発生していない場合は、復号装置１２００内の比較部１２４０の出力ｊは常に１である。

【００４９】

また、復号誤りが発生している場合に、復号装置１２００内の比較部１２４０の出力ｊが１となる確率、即ち、復号装置１２００内の第２の一方向性関数部１２２０によって生成されたｈ（ｍ’）が、暗号装置１１００内の第１の一方向性関数部１１２０によって生成されたｈ（ｍ）と偶然等しくなる確率は、出力がｋビットのハッシュ関数を第１の一方向性関数部１１２０、及び第２の一方向性関数部１２２０に用いた場合、ｋビットの出力は２＾ｋ通り存在するので、２＾（－ｋ）と等しい。ここで、ａ＾ｂはａをｂ乗した結果を表す。

【００５０】

従って、実際に復号誤りが発生したとき、復号装置１２００から出力されるｊを調べることによって、確率１－２＾（－ｋ）で復号誤りが発生したことを確認することができる。例えば、第１の一方向性関数部１１２０、及び第２の一方向性関数部１２２０で用いるハッシュ関数をＳＨＡ－１としたとき、ＳＨＡ－１は１６０ビットの出力を持つので、この確率は１－２＾（－１６０）となり、ほぼ復号誤りの発生を検出することができる。ＳＨＡ－１については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書、１９９７、１８９～１９５ページに詳しく述べられている。

【００５１】

また、通信量は、暗号化部１１１０の出力ビット長と第１の一方向性関数部１１２０の出力ビット長を合わせた量である。一般にハッシュ関数の出力ビット長は暗号文の出力ビット長よりも小さいので、この例での通信量は、暗号文の出力ビット長の２倍を越えない。例えば、ハッシュ関数にＳＨＡ－１を使った場合、現在、ＮＴＲＵ暗号方式を含む暗号方式は暗号文長が１６０ビット以上のものが使われることが多いので、このことは成り立つ。

【００５２】

従来例２のデータ暗号化システムの通信量は、暗号文の出力ビット長の複数倍であったので、従来例２のデータ暗号化システムに比べて、この例では通信量が少なくなり、通信効率が向上する。さらに、安全性については、ハッシュ関数は、出力の値から入力の値を得ることは困難であり、また、従来例２のように同じ

平文を複数回送信することはないので、十分な安全性が確保できる。

【００５３】

（実施の形態１の変形例）

以上、データ暗号化システムにおいて、暗号化部にＮＴＲＵ暗号方式を適用し、第１の一方向性関数部にハッシュ関数を用いる実施の形態に基づいて説明したが、本発明は、この実施の形態に限られず、暗号化部に、ＤＥＳ暗号方式、ＲＳＡ暗号方式やＥｌＧａｍａｌ暗号方式などの一般の暗号方式を適用でき、また第１の一方向性関数部には、ハッシュ関数以外に、前記一般の暗号方式の暗号化関数などの一方向性関数を用いてもよい。ＤＥＳ暗号方式、ＲＳＡ暗号方式、及びＥｌＧａｍａｌ暗号方式については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書、１９９７に詳しく述べられている。さらに、システム利用者全体で一方向性関数を共有せずに、送信側及び受信側のユーザ組毎に一方向性関数が異なっていてもよい。

【００５４】

また、本発明は、上記のデータ暗号化システムを実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラムまたは、前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリ、ＩＣカードなどに記録したものとしてもよい。

【００５５】

また、これらの記録媒体に記録されている前記コンピュータプログラムまたは、前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワークなどを経由して伝送するものとしてもよい。

【００５６】

（実施の形態２）

図６は、実施の形態２における復号誤りが発生し得る暗号方式における復号誤

り検出が可能であるデータ暗号化システム２０００の構成を示すブロック図である。

【００５７】

（データ暗号化システム２０００の構成）

データ暗号化システム２０００は、復号誤りが発生し得る暗号方式における復号誤り検出が可能であるシステムであり、暗号装置２１００、復号装置２２００、及び通信路２３００から構成される。ここでは、復号誤りが発生し得る暗号方式として、ＮＴＲＵ暗号方式を用いた構成例を与える。

【００５８】

（暗号装置２１００の構成）

図７は、暗号装置２１００の構成を示すブロック図である。暗号装置２１００は、暗号化部２１１０、第１の一方向性関数部２１２０、送信部２１３０及び情報付加部２１４０を備える。ここでは、暗号化部２１１０としてＮＴＲＵ暗号方式を用い、第１の一方向性関数部２１２０としてハッシュ関数を用い、情報付加部２１４０として予め決められたビット数の乱数を付加する情報付加部を用いた構成例を与える。

【００５９】

暗号装置２１００は、平文ｍを入力とし、ｍに対する第１の暗号部分情報である、ＮＴＲＵ暗号方式による暗号文ｃ（＝Ｅ（ｍ｜｜Ｒａ，Ｋｐ，ｒ））と第２の暗号部分情報であるハッシュ関数値ｈ（ｍ）を連結して出力する。

【００６０】

（暗号化部２１１０）

図８は、暗号化部２１１０の構成を示すブロック図である。暗号化部２１１０は、ＮＴＲＵ暗号方式の暗号化を行うものであり、暗号化関数部２１１１及び乱数生成部２１１２を備え、予め暗号化に用いる暗号鍵Ｋｐが与えられているものとする。暗号化部２１１０は、情報付加部２１４０から入力として平文ｍ｜｜Ｒａが与えられたとき、乱数生成部２１１２で乱数ｒを生成し、予め与えられた暗号鍵Ｋｐを用いて暗号化する際に、乱数ｒをパラメータとして使用して、平文ｍ｜｜Ｒａを暗号化関数部２１１１で暗号化した結果Ｅ（ｍ｜｜Ｒａ，Ｋｐ，ｒ）

を生成し、送信部２１３０に出力する。

【００６１】

以下、実施の形態２において、

ｃ＝Ｅ（ｍ｜｜Ｒａ，Ｋｐ，ｒ）

とする。ここで、上記乱数の例としては、Ｃ言語のライブラリ関数であるｒａｎｄ（）が挙げられる。

【００６２】

（第１の一方向性関数部２１２０）

第１の一方向性関数部２１２０は、予め一方向性関数としてハッシュ関数ｈが与えられているものとする。第１の一方向性関数部２１２０は、上記平文ｍのハッシュ関数ｈの値ｈ（ｍ）を生成し、送信部２１３０に出力する。ここで用いるハッシュ関数ｈは、関数の値ｈ（ｍ）から平文ｍの値を得ることが困難であるような十分に安全なもので、かつ衝突困難なものとする。

【００６３】

（送信部２１３０）

送信部２１３０は、暗号化部２１１０から出力された暗号文ｃと第１の一方向性関数部２１２０から出力されたｈ（ｍ）を連結して通信路２３００に送信する。

【００６４】

（情報付加部２１４０）

情報付加部２１４０は、入力ｍが与えられたとき、予め決められたビット数ｒＬｅｎの長さの乱数Ｒａを生成して、ｍにＲａをビット結合した結果ｍ｜｜Ｒａを算出し、暗号化部２１１０に入力する。ここで、ビット結合という操作は、２つの値をビット列で表現し、それらを結合したものを１つの値とする操作である。例えば、ｍ＝１０、ｒＬｅｎ＝５、Ｒａ＝７とすると、ｍのビット列表現は１０１０、Ｒａの長さｒＬｅｎのビット列表現は００１１１となるので、ビット結合した結果は、１０１０００１１１となり、これは十進数で３２７である。

【００６５】

（復号装置２２００の構成）

図９は、復号装置２２００の構成を示すブロック図である。復号装置２２００は、入力として暗号文ｃとハッシュ関数値ｈ（ｍ）を受け取り、復号文ｍ’と復号誤り検出結果ｊを出力する。復号装置２２００は、復号化部２２１０、第２の一方向性関数部２２２０、受信部２２３０、比較部２２４０、及び情報除去部２２５０を備える。

【００６６】

（復号化部２２１０）

図１０は、復号化部２２１０の構成を示すブロック図である。復号化部２２１０は、暗号化部２１１０で用いられた暗号方式の復号を行うものであり、復号化関数部２２１１を備え、予め復号に用いる復号鍵Ｋｓが与えられているものとする。復号化部２２１０は、入力として上記暗号文ｃが与えられたとき、予め与えられた復号鍵Ｋｓを用いて、暗号文ｃを復号化関数部２２１１で復号した結果Ｄ（ｃ，Ｋｓ）を生成し、情報除去部２２５０へ入力する。以下、実施の形態２において、

Ｍａ＝Ｄ（ｃ，Ｋｓ）

とする。

【００６７】

（第２の一方向性関数部２２２０）

第２の一方向性関数部２２２０は、第１の一方向性関数部２１２０と同じ動作を行うものであり、予め一方向性関数としてハッシュ関数ｈが与えられているものとする。第２の一方向性関数部２２２０は、情報除去部２２５０によって入力されたｍ’のハッシュ関数ｈの値ｈ（ｍ’）を生成し、比較部２２４０に出力する。

【００６８】

（受信部２２３０）

受信部２２３０は、通信路２３００から連結された入力ｃ，ｈ（ｍ）を受け取り、ｃを復号化部２２１０に、ｈ（ｍ）を比較部２２４０にそれぞれ入力する。

【００６９】

（比較部２２４０）

比較部２２４０は、ｈ（ｍ）とｈ（ｍ’）を入力として、ｈ（ｍ）とｈ（ｍ’）が等しいかどうか比較し、等しい場合はｊ＝１とし、等しくない場合はｊ＝０をとして、比較結果ｊを出力する。

【００７０】

（情報除去部２２５０）

情報除去部２２５０は、復号化部２２１０より入力Ｍａが与えられたとき、Ｍａをビット列表現した結果から情報付加部２１４０で用いられたビット数ｒＬｅｎのビットを除去した結果を算出し、第２の一方向性関数部２２２０に入力する。例えば、Ｍａ＝３２７、ｒＬｅｎ＝５とすると、Ｍａのビット列表現は１０１０００１１１となり、これから長さｒＬｅｎのビット００１１１を除去すると、結果は１０１０となり、これは十進数で１０である。

【００７１】

（通信路２３００の構成）

通信路２３００は、暗号装置２１００と復号装置２２００との間のデータのやり取りが可能であるような通信路である。例えば、無線通信路やインターネットである。

【００７２】

（データ暗号化システム２０００の動作）

データ暗号化システム２０００の全体の動作について、図６、図７、図９と、以下に述べる処理順序を用いて説明する。ここで、暗号鍵Ｋｐ、復号鍵Ｋｓ、及び一方向性関数ｈは予め適切な方法で生成され、暗号鍵Ｋｐは暗号化部２１１０に格納され、復号鍵Ｋｓは復号化部２２１０に格納され、一方向性関数ｈは第１の一方向性関数部２１２０及び第２の一方向性関数部２２２０に与えられているものとする。

【００７３】

暗号装置２１００は、入力として平文ｍを受け取る（ステップＳ２０１）。情報付加部２１４０は、入力されたｍに対しｍ｜｜Ｒａを生成し、暗号化部２１１０に入力する（ステップＳ２０２）。暗号化部２１１０は、入力されたｍ｜｜Ｒａに対し、ｃ＝Ｅ（ｍ｜｜Ｒａ，Ｋｐ，ｒ）を生成し、送信部２１３０に入力す

る（ステップＳ２０３）。第１の一方向性関数部２１２０は、入力されたｍに対し、ｈ（ｍ）を生成し、送信部２１３０に入力する（ステップＳ２０４）。送信部２１３０は、入力されたｃ、及びｈ（ｍ）を連結して暗号文とし、通信路２３００に送信する（ステップＳ２０５）。

【００７４】

受信部２２３０は、通信路２３００から暗号文である連結されたｃ、及びｈ（ｍ）を受信し、ｃを復号化部２２１０に、ｈ（ｍ）を比較部２２４０にそれぞれ入力する（ステップＳ２０６）。復号化部２２１０は、入力されたｃに対し、Ｍａ＝Ｄ（ｃ，Ｋｓ）を生成し、情報除去部２２５０に入力する（ステップＳ２０７）。情報除去部２２５０は、入力されたＭａに対し、ｍ’を生成し、第２の一方向性関数部２２２０に入力する（ステップＳ２０８）。第２の一方向性関数部２２２０は、入力されたｍ’に対し、ｈ（ｍ’）を生成し、比較部２２４０に入力する（ステップＳ２０９）。比較部２２４０は、入力されたｈ（ｍ’）とｈ（ｍ）が等しいかどうか判定し、等しい場合ｊ＝１、等しくない場合ｊ＝０として、比較結果ｊを出力する（ステップＳ２１０）。

【００７５】

復号装置２２００は、情報除去部２２５０で出力されたｍ’と比較部２２４０で出力されたｊを復号文として出力する（ステップＳ２１１）。

【００７６】

（実施の形態２における動作検証と従来例との比較）

以下に、この例の復号誤りの検出について説明する。以下で従来の方法との比較を行う。この例では、復号誤りが発生していない場合は、復号装置２２００内の比較部２２４０の出力ｊは常に１である。

【００７７】

また、復号誤りが発生している場合に、復号装置２２００内の比較部２２４０の出力ｊが１となる確率、即ち、復号装置２２００内の第２の一方向性関数部２２２０によって生成されたｈ（ｍ’）が、暗号装置２１００内の第１の一方向性関数部２１２０によって生成されたｈ（ｍ）と偶然等しくなる確率は、出力がｋビットのハッシュ関数を第１の一方向性関数部２１２０、及び第２の一方向性関

数部２２２０に用いた場合、ｋビットの出力は２＾ｋ通り存在するので、２＾（－ｋ）と等しい。

【００７８】

従って、実際に復号誤りが発生したとき、復号装置２２００から出力されるｊを調べることによって、確率１－２＾（－ｋ）で復号誤りが発生したことを確認することができる。例えば、第１の一方向性関数部２１２０、及び第２の一方向性関数部２２２０で用いるハッシュ関数をＳＨＡ－１としたとき、ＳＨＡ－１は１６０ビットの出力を持つので、この確率は１－２＾（－１６０）となり、ほぼ復号誤りの発生を検出することができる。

【００７９】

また、通信量は、暗号化部２１１０の出力ビット長と第１の一方向性関数部２１２０の出力ビット長を合わせた量である。一般にハッシュ関数の出力ビット長は暗号文の出力ビット長よりも小さいので、この例での通信量は、暗号文の出力ビット長の２倍を越えない。例えば、ハッシュ関数にＳＨＡ－１を使った場合、現在、ＮＴＲＵ暗号方式を含む暗号方式は暗号文長が１６０ビット以上のものが使われることが多いので、このことは成り立つ。

【００８０】

従来例２のデータ暗号化システムの通信量は、暗号文の出力ビット長の複数倍であったので、従来例２のデータ暗号化システムに比べて、この例では通信量が少なくなり、通信効率が向上する。

【００８１】

ここで、平文ｍは、長さｒＬｅｎの乱数Ｒａが付加されて、暗号化部２１１０に入力されるので、暗号装置２１００に入力できる平文の長さは、実施の形態１のデータ暗号化システムよりも長さｒＬｅｎだけ短くなる。但し、暗号化部２１１０に暗号文長が１６０ビットの暗号方式を用いるとき、ｒＬｅｎを３２ビットとしても、１２８ビットのデータを送信できるため、実用上は問題ない。

【００８２】

さらに、安全性については、ハッシュ関数は、出力の値から入力の値を得ることは困難であり、また、従来例２のように同じ平文を複数回送信することはない

ので、十分な安全性が確保できる。加えて、復号誤り検出の後に、再送要求を行い、同じデータを再度送信させるプロトコルを考えたときでも、平文に乱数が付加されて暗号化されているので、従来例２のMultiple Transmission Attackに対して、この例では従来例２のデータ暗号化システムよりも耐性を持っている。

【００８３】

（実施の形態２の変形例）

以上、データ暗号化システムにおいて、暗号化部にＮＴＲＵ暗号方式を適用し、第１の一方向性関数部にハッシュ関数を用い、情報付加部で乱数を付加する処理を行う実施の形態に基づいて説明したが、本発明は、この実施の形態に限られず、暗号化部に、ＤＥＳ暗号方式、ＲＳＡ暗号方式やＥｌＧａｍａｌ暗号方式などの一般の暗号方式を適用でき、また第１の一方向性関数部には、ハッシュ関数以外に、前記一般の暗号方式の暗号化関数などの一方向性関数を用いてもよい。加えて、情報付加部では、時間情報や定型情報など、任意の情報を付加する処理を行ってもよい。ＤＥＳ暗号方式、ＲＳＡ暗号方式、及びＥｌＧａｍａｌ暗号方式については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書、１９９７に詳しく述べられている。さらに、システム利用者全体で一方向性関数を共有せずに、送信側及び受信側のユーザ組毎に一方向性関数が異なっていてもよい。

【００８４】

また、本発明は、上記の公開鍵暗号方法を実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラムまたは、前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリ、ＩＣカードなどに記録したものとしてもよい。

【００８５】

また、これらの記録媒体に記録されている前記コンピュータプログラムまたは、前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、

インターネットを代表とするネットワークなどを経由して伝送するものとしてもよい。

【００８６】

【発明の効果】

以上に説明したように本発明は、従来例における問題点を鑑みて行われたもので、復号誤りの発生し得る暗号方式において、安全で、効率的に、かつほぼ完全に復号誤りの検出が可能となった。以上により、実用的な復号誤りの検出装置を提供することができ、その価値は大きい。

【図面の簡単な説明】

【図１】

本発明の実施の形態１のデータ暗号化システムのブロック図

【図２】

本発明の実施の形態１の暗号装置のブロック図

【図３】

本発明の実施の形態１の暗号化部のブロック図

【図４】

本発明の実施の形態１の復号装置のブロック図

【図５】

本発明の実施の形態１の復号化部のブロック図

【図６】

本発明の実施の形態２のデータ暗号化システムのブロック図

【図７】

本発明の実施の形態２の暗号装置のブロック図

【図８】

本発明の実施の形態２の暗号化部のブロック図

【図９】

本発明の実施の形態２の復号装置のブロック図

【図１０】

本発明の実施の形態２の復号化部のブロック図

【図１１】

従来例１のデータ暗号化システムのブロック図

【図１２】

従来例１の暗号装置のブロック図

【図１３】

従来例１の暗号化部のブロック図

【図１４】

従来例１の復号装置のブロック図

【図１５】

従来例１の復号化部のブロック図

【図１６】

従来例２のデータ暗号化システムのブロック図

【図１７】

従来例２の暗号装置のブロック図

【図１８】

従来例２の暗号化部のブロック図

【図１９】

従来例２の復号装置のブロック図

【図２０】

従来例２の復号化部のブロック図

【符号の説明】

１０００，２０００，３０００，４０００　データ暗号化システム

１１００，２１００，３１００，４１００　暗号装置

１１１０，２１１０，３１１０，４１１０　暗号化部

１１１１，２１１１，３１１１，４１１１　暗号化関数部

１１１２，２１１２，３１１２，４１１２　乱数生成部

１１２０，２１２０　第１の一方向性関数部

１１３０，２１３０，３１２０，４１２０　送信部

１２００，２２００，３２００，４２００　復号装置

１２１０，２２１０，３２１０，４２１０　復号化部

１２１１，２２１１，３２１１，４２１１　復号化関数部

１２２０，２２２０　第２の一方向性関数部

１２３０，２２３０，３２２０，４２２０　受信部

１２４０，２２４０，４２３０　比較部

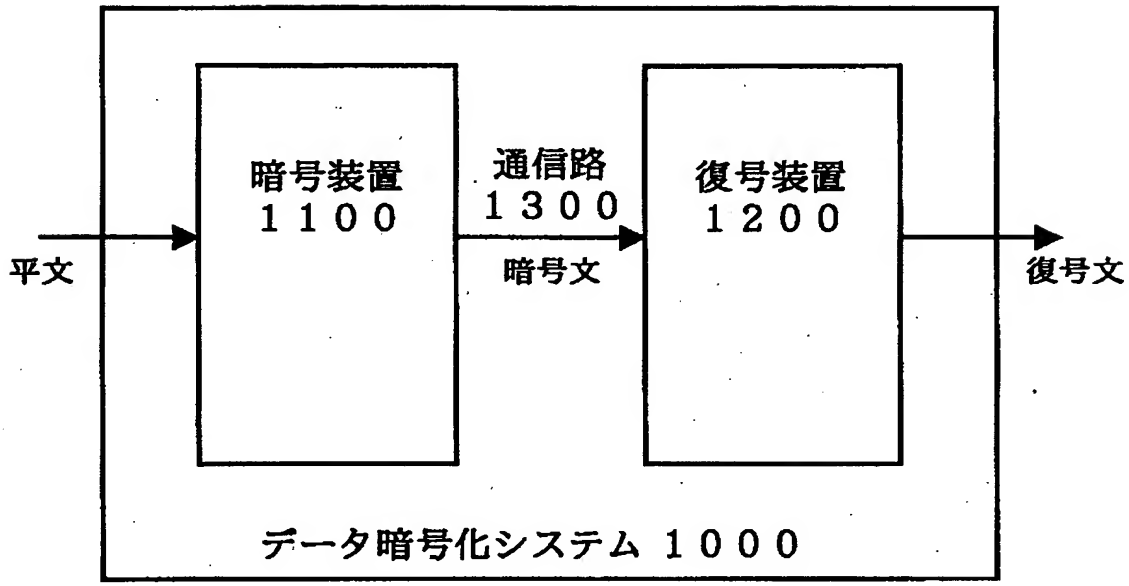
１３００，２３００，３３００，４３００　通信路

２１４０　情報付加部

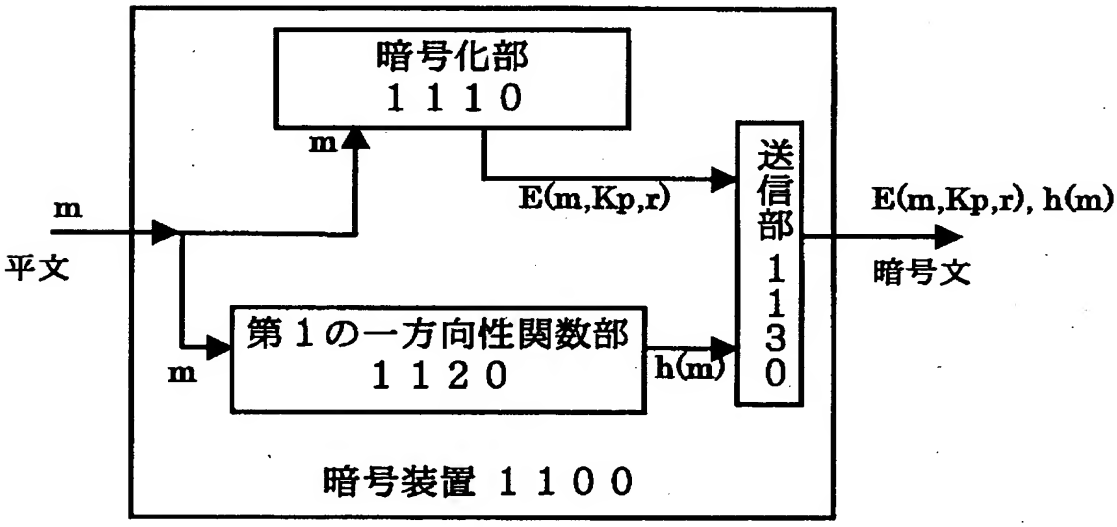
２２５０　情報除去部

【書類名】　　図面

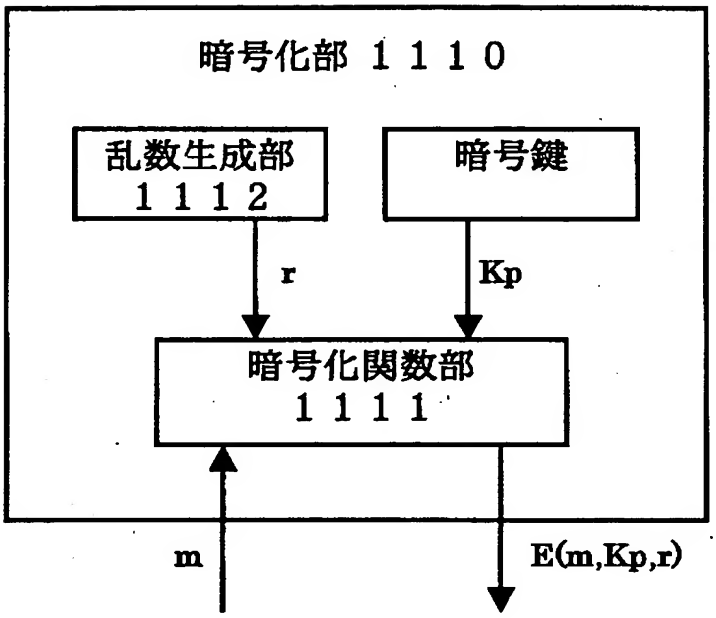
【図１】


暗号装置
１１００
通信路
１３００
復号装置
１２００
平文
暗号文
復号文
データ暗号化システム １０００

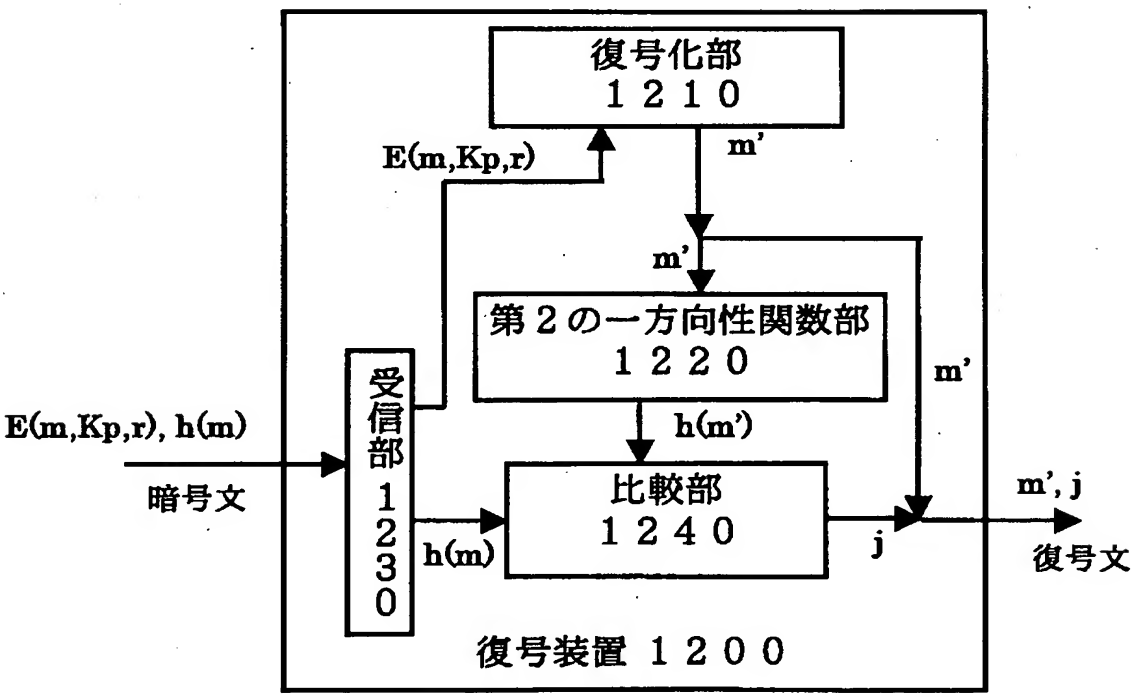
【図２】


暗号化部
１１１０
m
E(m,Kp,r)
送信部１１３０
E(m,Kp,r), h(m)
m
平文
暗号文
m
第１の一方向性関数部
１１２０
h(m)
暗号装置 １１００

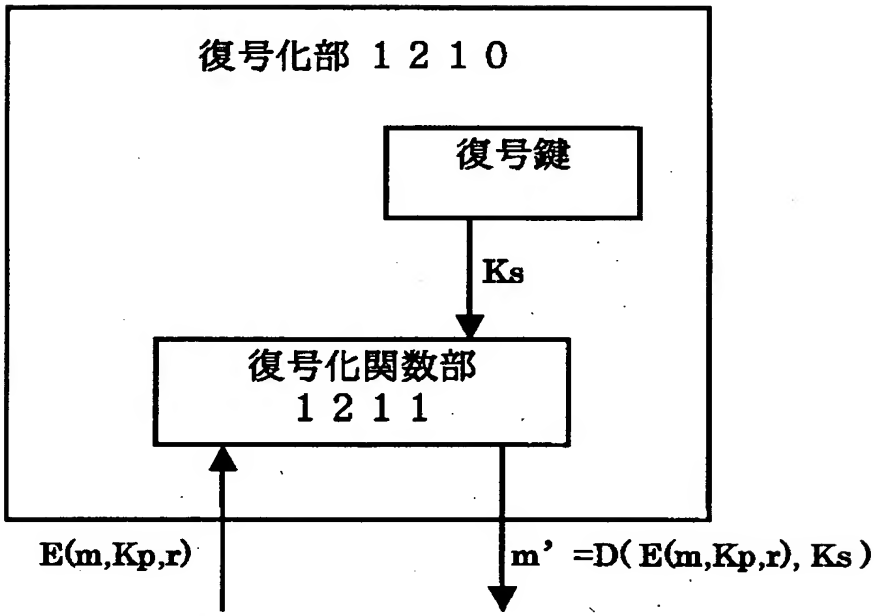
【図３】


暗号化部 １１１０
乱数生成部
１１１２
暗号鍵
r
Kp
暗号化関数部
１１１１
m
E(m,Kp,r)

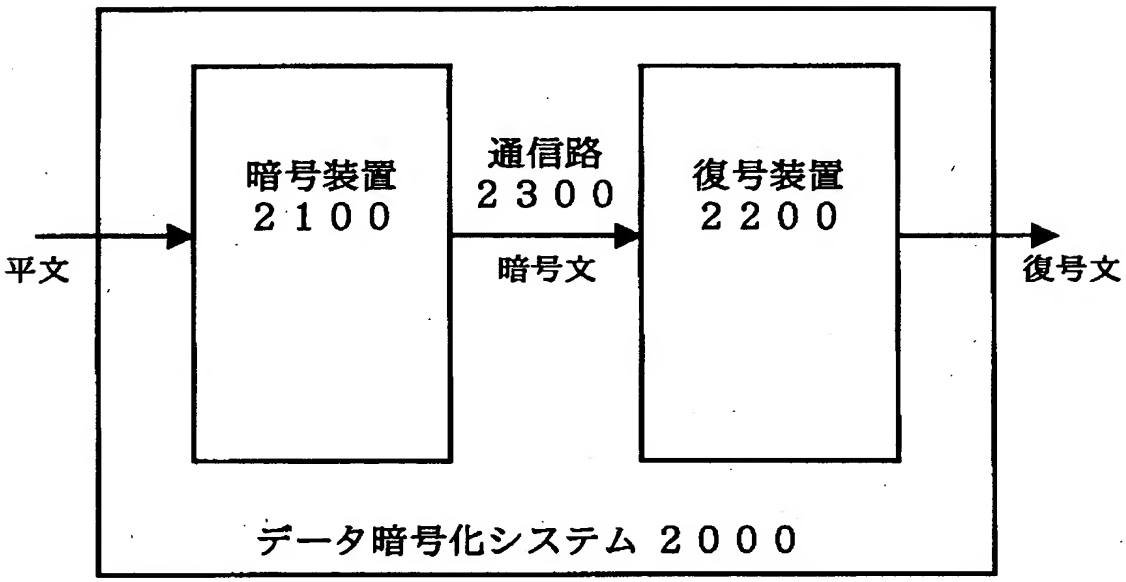
【図４】


復号化部
１２１０
E(m,Kp,r)
m'
m'
第２の一方向性関数部
１２２０
m'
E(m,Kp,r), h(m)
暗号文
受信部
１２３０
h(m')
比較部
１２４０
m', j
h(m)
j
復号文
復号装置 １２００

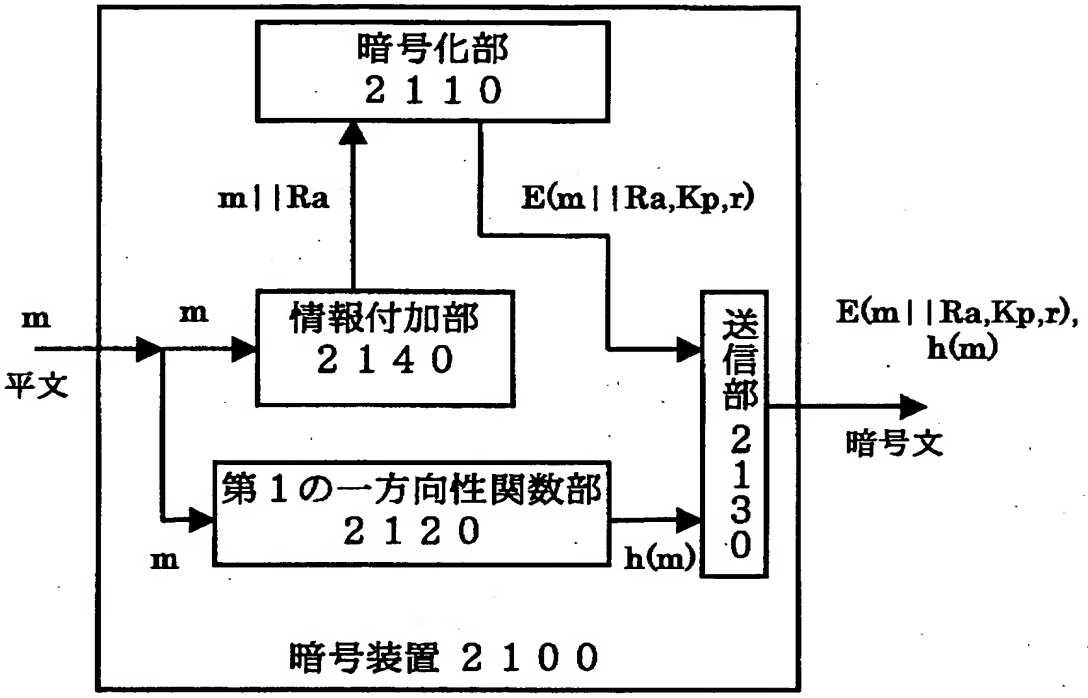
【図５】


復号化部 １２１０
復号鍵
Ks
復号化関数部
１２１１
E(m,Kp,r)
m’ =D( E(m,Kp,r), Ks )

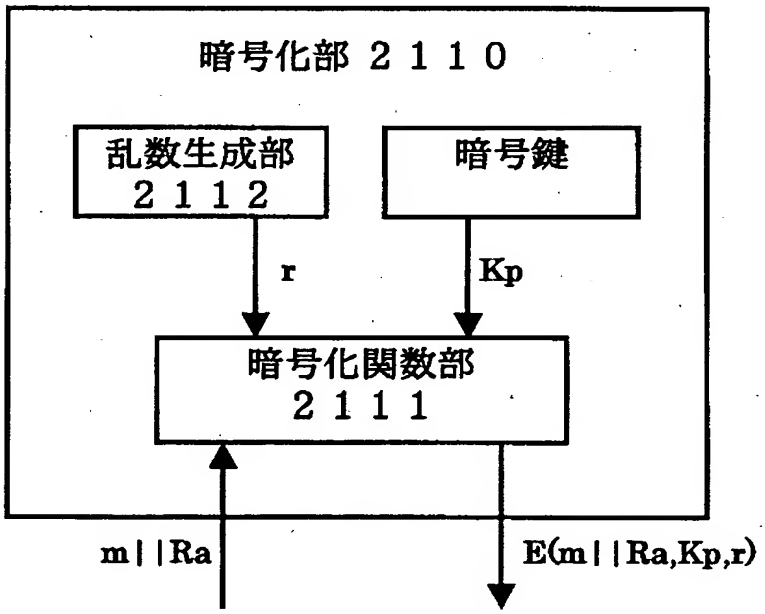
【図６】


暗号装置
２１００
通信路
２３００
復号装置
２２００
平文
暗号文
復号文
データ暗号化システム ２０００

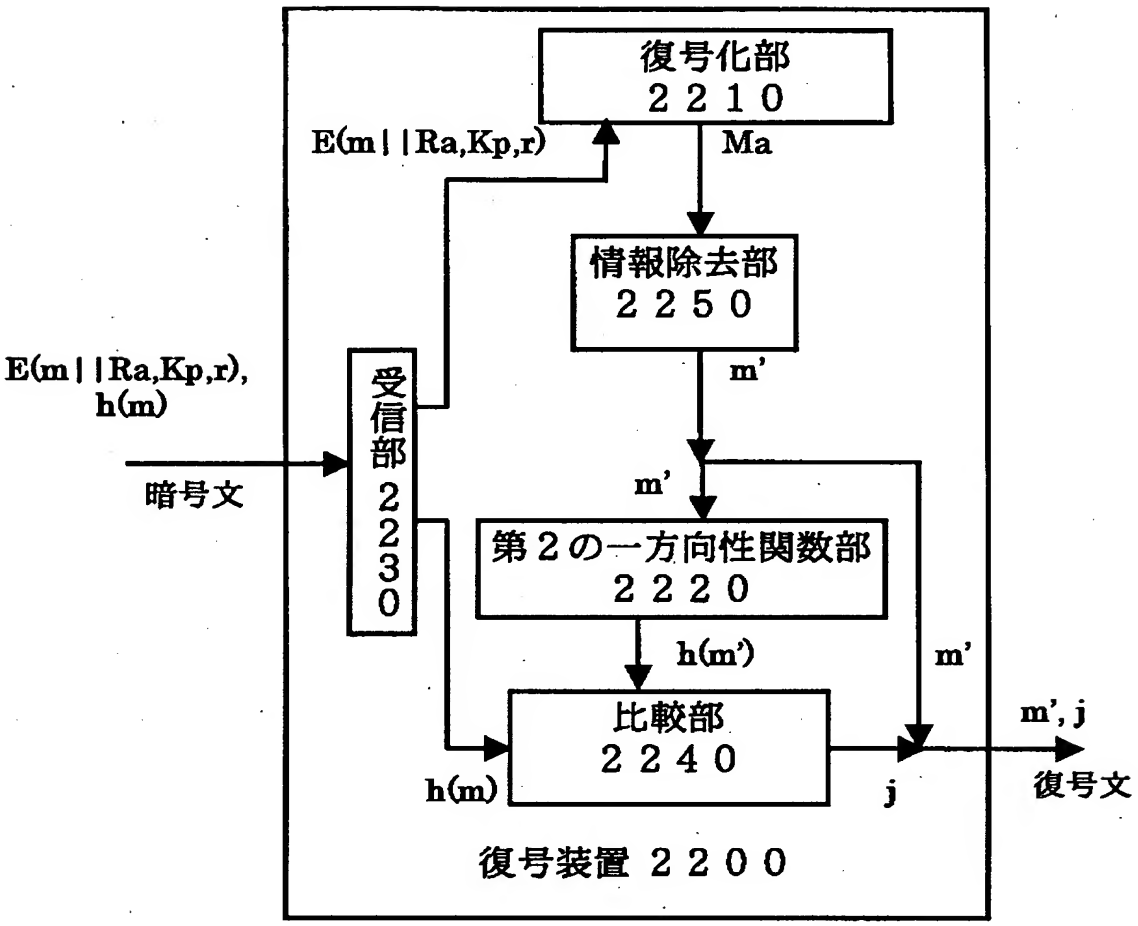
【図７】


暗号化部
２１１０
m||Ra
E(m||Ra,Kp,r)
m
平文
m
情報付加部
２１４０
送信部
２１３０
E(m||Ra,Kp,r),
h(m)
暗号文
第１の一方向性関数部
２１２０
m
h(m)
暗号装置 ２１００

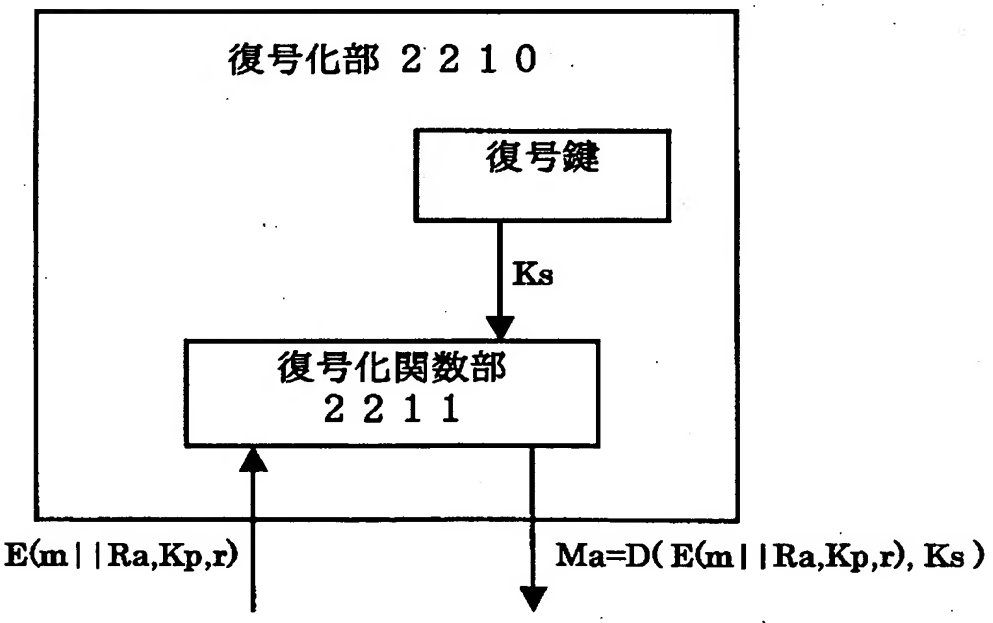
【図８】


暗号化部 ２１１０
乱数生成部
２１１２
暗号鍵
r
Kp
暗号化関数部
２１１１
m||Ra
E(m||Ra,Kp,r)

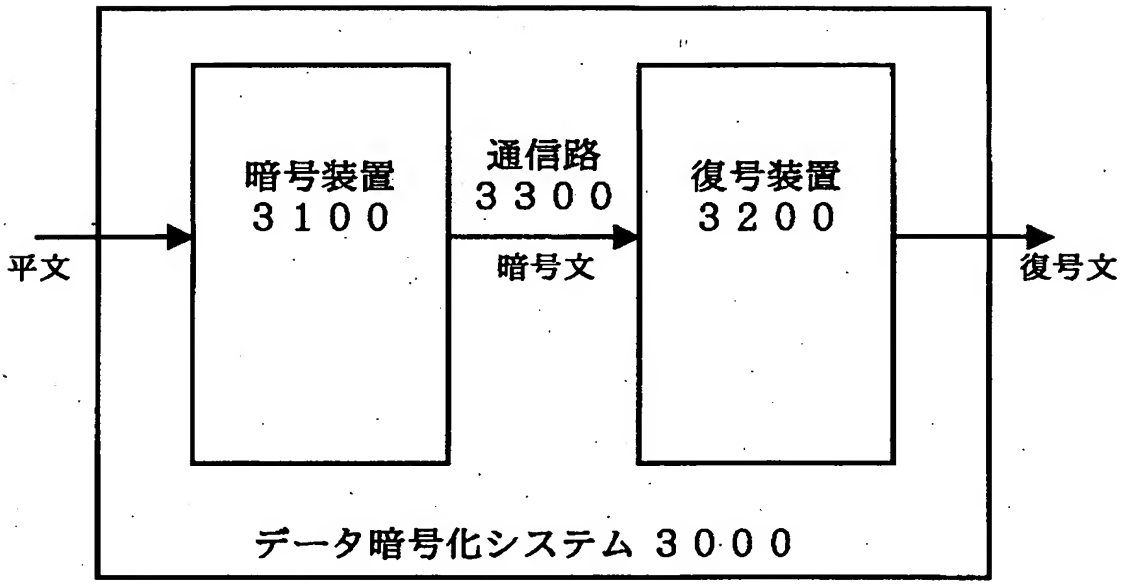
【図９】


復号化部
２２１０
E(m||Ra,Kp,r)
Ma
情報除去部
２２５０
m'
E(m||Ra,Kp,r),
h(m)
暗号文
受信部
２２３０
m'
第２の一方向性関数部
２２２０
h(m')
m'
比較部
２２４０
m', j
h(m)
j
復号文
復号装置 ２２００

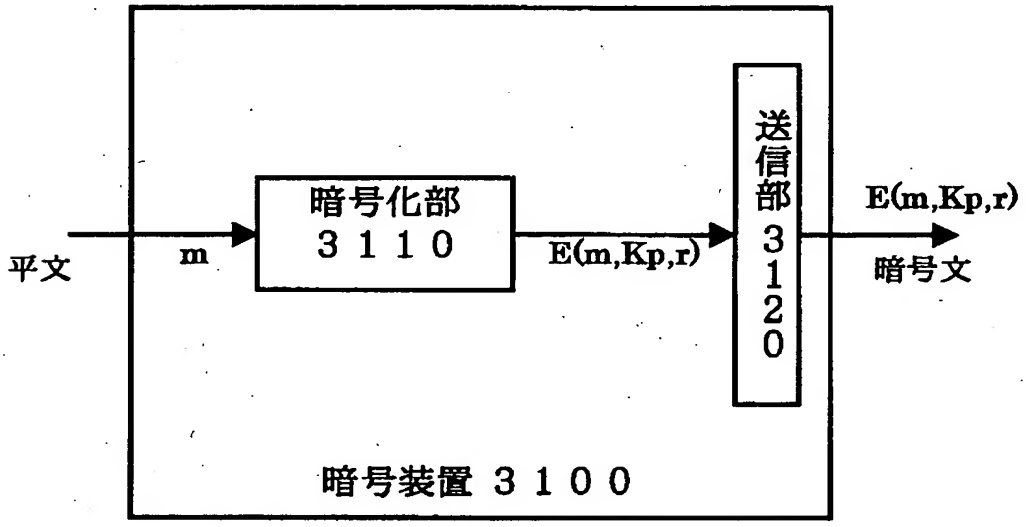
【図１０】


復号化部 ２２１０
復号鍵
Ks
復号化関数部
２２１１
E(m||Ra,Kp,r)
Ma=D( E(m||Ra,Kp,r), Ks )

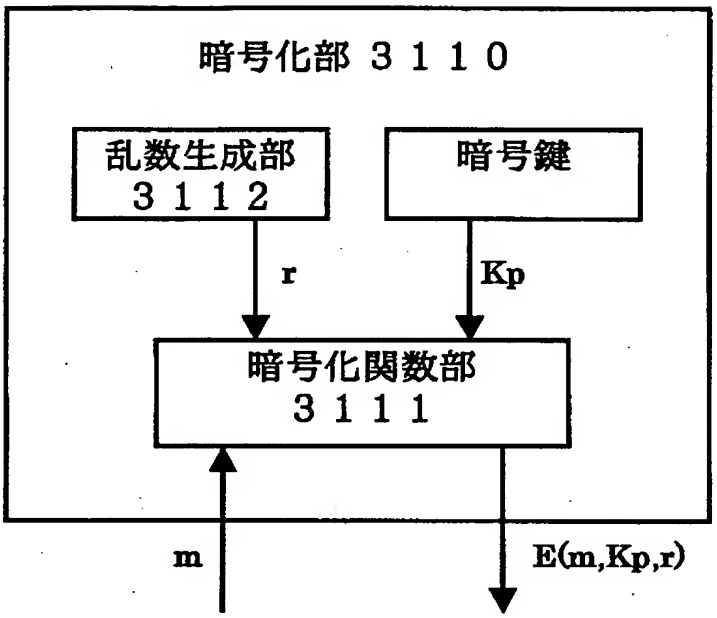
【図１１】


暗号装置
３１００
通信路
３３００
復号装置
３２００
平文
暗号文
復号文
データ暗号化システム ３０００

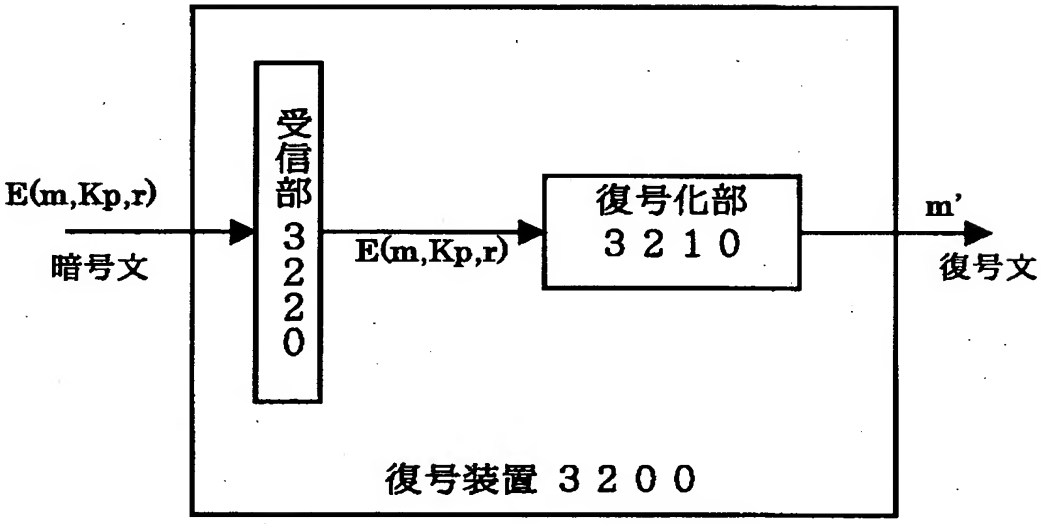
【図１２】


暗号化部
３１１０
送信部
３１２０
平文
m
E(m,Kp,r)
E(m,Kp,r)
暗号文
暗号装置 ３１００

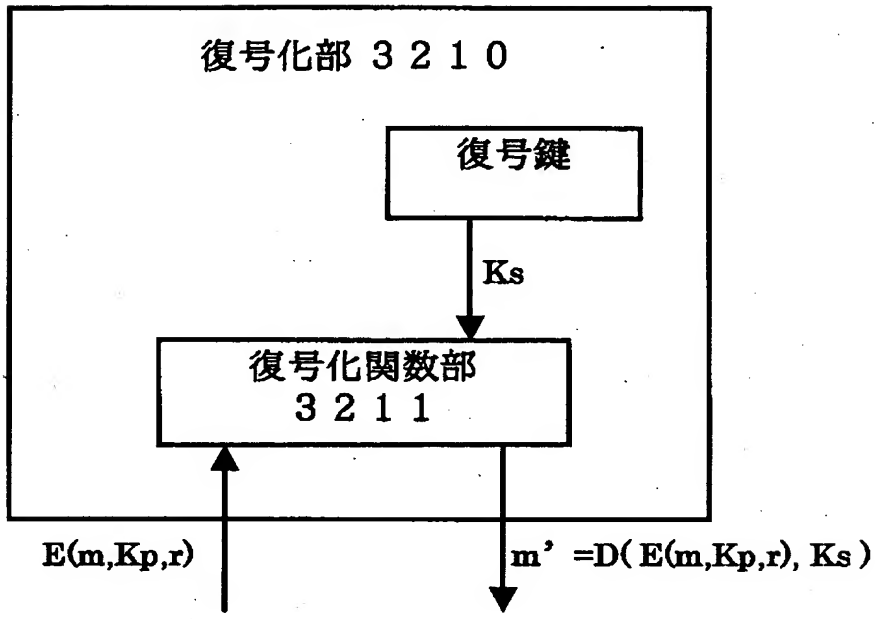
【図１３】


暗号化部 ３１１０
乱数生成部
３１１２
暗号鍵
r
Kp
暗号化関数部
３１１１
m
E(m,Kp,r)

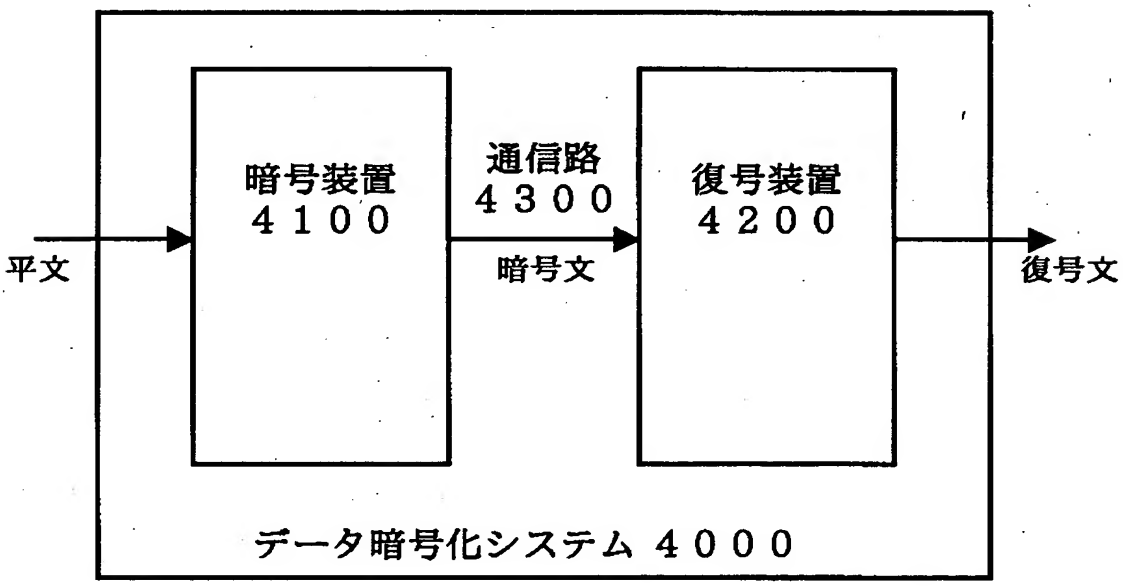
【図１４】


E(m,Kp,r)
暗号文
受信部
３２２０
E(m,Kp,r)
復号化部
３２１０
m'
復号文
復号装置 ３２００

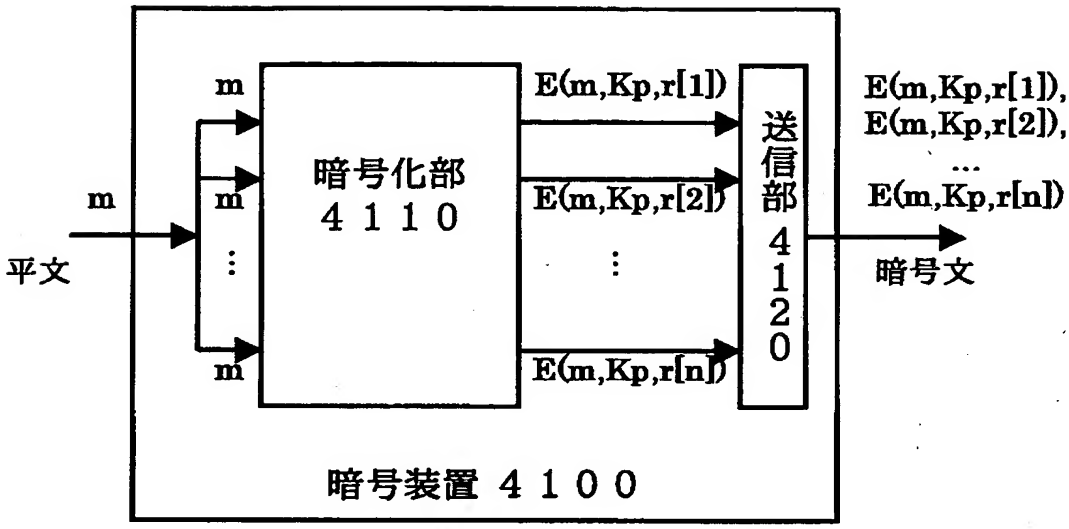
【図１５】


復号化部 ３２１０
復号鍵
Ks
復号化関数部
３２１１
E(m,Kp,r)
m' =D( E(m,Kp,r), Ks )

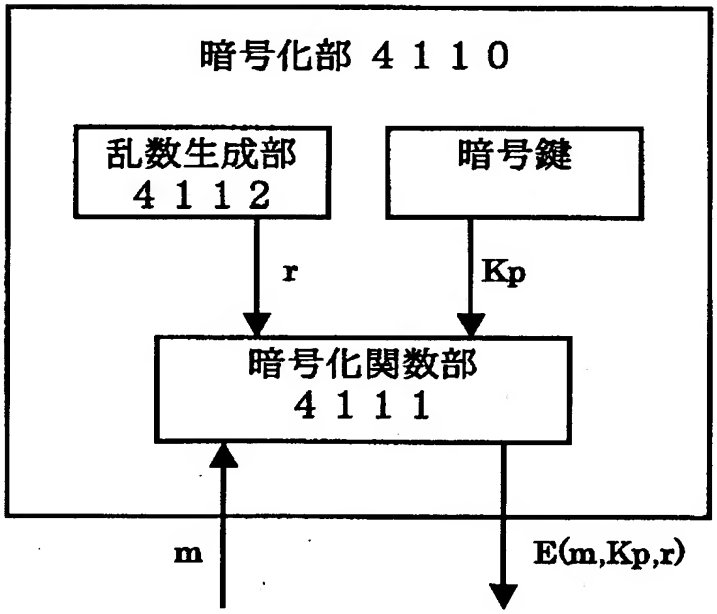
【図１６】


暗号装置
４１００
通信路
４３００
復号装置
４２００
平文
暗号文
復号文
データ暗号化システム ４０００

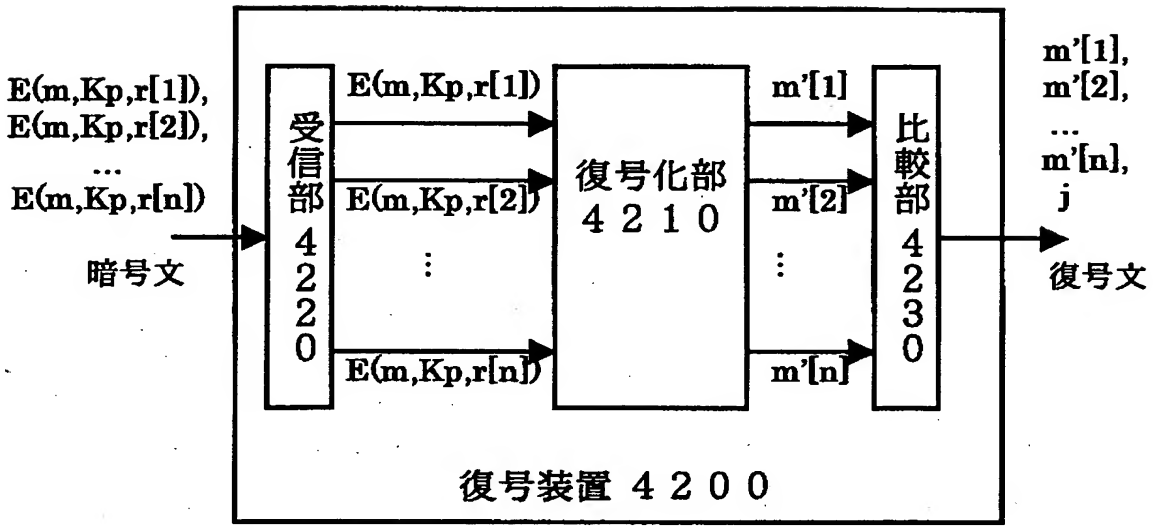
【図１７】


m
m
m
暗号化部
４１１０
E(m,Kp,r[1])
E(m,Kp,r[2])
E(m,Kp,r[n])
送信部
４１２０
E(m,Kp,r[1]),
E(m,Kp,r[2]),
…
E(m,Kp,r[n])
平文
暗号文
暗号装置 ４１００

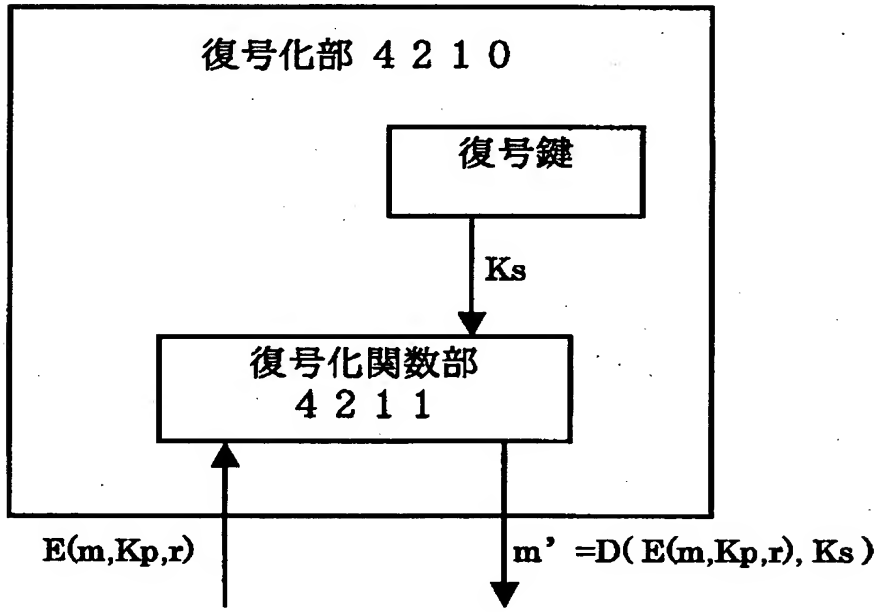
【図１８】


暗号化部 ４１１０
乱数生成部
４１１２
暗号鍵
r
Kp
暗号化関数部
４１１１
m
E(m,Kp,r)

【図１９】


E(m,Kp,r[1]),
E(m,Kp,r[2]),
…
E(m,Kp,r[n])
暗号文
受信部 4220
E(m,Kp,r[1])
E(m,Kp,r[2])
E(m,Kp,r[n])
復号化部 4210
m'[1]
m'[2]
m'[n]
比較部 4230
m'[1],
m'[2],
…
m'[n],
j
復号文
復号装置 4200

【図２０】


復号化部 4210
復号鍵
Ks
復号化関数部 4211
E(m,Kp,r)
m' =D( E(m,Kp,r), Ks )

【書類名】　要約書

【要約】

【課題】　データ暗号化システムにより、安全で効率的に復号誤りを検出する技術を提供することを目的とする。

【解決手段】　本発明は、送信側と受信側で予め対となる暗号鍵と復号鍵、また一方向性関数を定めておき、送信側で平文を、暗号鍵と一方向性関数に基づき暗号化して暗号文を生成し、暗号文を受信側に送信し、受信側では復号鍵と一方向性関数に基づいて暗号文を復号し、復号文を入手することを特徴とする。

【選択図】　図１

# 出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社